Analyse des systèmes

Sûreté de fonctionnement

Introduction

La complexité croissante des organisations et systèmes industriels et la recherche récurrente d'une meilleure compétitivité forcent les entreprises et gestionnaires d'équipements à une évaluation systématique et quasi continue des performances.
La performance est multidimensionnelle. Déclinée suivant des attributs de coût, qualité, délai,…, des critères de productivité, flexibilité, robustesse,…, des aspects environnementaux, sociaux, sociétaux,…, elle doit être évaluée sur l'ensemble du cycle de vie du système ou des produits réalisés.
Cette diversité, motivée par une logique socio-économique de développement durable, génère un besoin fort en méthodologies, techniques et outils pour aider aux choix des décideurs dans les phases de conception, de développement ou d'exploitation des produits et systèmes.
Nombreuses sont les réponses ; nombreux aussi sont les ouvrages et articles spécialisés qui exposent celles-ci, depuis un état détaillé de toutes les formes d'aide jusqu'à la présentation précise d'outil ou de technique particulière.

L'objectif de ce chapitre est de fournir une approche efficace d'analyse d'un système afin d'estimer et d'évaluer la performance de celui-ci.
Les éléments méthodologiques qui garantissent une analyse rationnelle du système et de ses performances seront mis en exergue, focalisant sur les aspects sûreté de fonctionnement considérés dès les étapes de conception ; la recherche de performance est, en effet, corrélée au souci constant d'amélioration de la disponibilité opérationnelle du système et d'optimisation de son coût global de possession.

Le chapitre est organisé en cinq parties.
La notion de système est d'abord discutée. Prenant appui sur les différentes vues descriptives d'un système, il est précisé l'approche à suivre pour en faire une analyse efficace. Par la suite, l'angle considéré est celui d'une démarche systémique d'analyse.

La notion de performance de système et celle de mesure de cette performance sont présentées dans le deuxième paragraphe. Allant directement au cœur des problèmes d'évaluation de la performance, il est mis en exergue la position de la sûreté de fonctionnement dans l'obtention de la performance.

Dans le paragraphe suivant, les principales méthodes d'analyse qui permettent la description et la représentation du fonctionnement du système sont rapidement présentées. Ces méthodes préparent à l'évaluation de la performance fonctionnelle et à l'estimation prévisionnelle des risques. Cet état a été limité à quelques outils illustratifs, d'usage courant, focalisant sur la position prise par ces outils dans le processus général d'analyse et, sur un plan particulier, la mise en relief de la présence de paramètres incertains, prépondérants dans les premières étapes du cycle de vie du produit ou du système.

Les principes de traitement de l'incertitude en modélisation et évaluation sont exposés dans le quatrième paragraphe suivis d'une présentation de ceux de l'analyse prévisionnelle des risques. Le paragraphe contient les éléments clefs qui guideront le choix des outils d'analyse et les traitements qui suivront.

Le paragraphe suivant est dédié à la présentation des méthodes d'évaluation de la sûreté de fonctionnement et d'analyse des risques pouvant être utilisées dès les étapes de conception. Là encore, il a été choisi de limiter ce recensement à des outils d'usage industriel ; cet état constitue donc une collection non exhaustive mais bien identifiable pour l'utilisateur. Rebouclant avec les propositions du début du chapitre, il est montré dans la comment ancrer les résultats fournis par ces méthodes à la définition du système tant en conception qu'en exploitation pour en améliorer les performances sur les phases utiles de son cycle de vie.

1 Notion de système

1.1 Système et système complexe

De nombreuses définitions ont été données dans la littérature scientifique et dans différents domaines pour établir la notion de système. Beaucoup se valent ; on retiendra celle, ancienne, proposée par Vesely et all [1] qui présentent un système comme un "ensemble déterminé d'éléments discrets (composants, constituants) interconnectés ou en interaction".
Cette définition a l'avantage d'une certaine généricité et pourra être étendue pour exprimer la complexité du système.
Formé d'éléments en interaction dynamique, un système correspond à une portion d'entité réelle, définie par une frontière établie en fonction d'un but, qui se distingue de son contexte ou de son milieu tout en procédant à des échanges avec son environnement [2].
Un système industriel, par exemple, réunira l'ensemble des moyens nécessaires pour créer la valeur ajoutée industrielle d'un produit ; il sera caractérisé par rapport à cette valeur ajoutée, aux flux qui le parcourent ainsi qu'aux aspects temporels, économiques, environnementaux,..., autant d'éléments sur lesquels est généralement attendu un niveau de performance.

Un système peut être considéré de plusieurs façons :

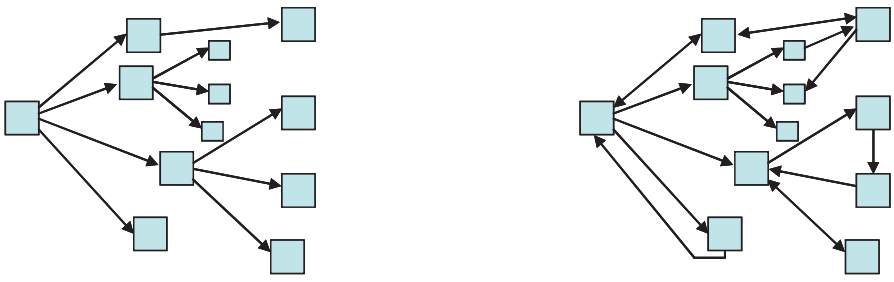
1) depuis son environnement, comme élément spécifique de type « boîte noire » avec des entrées et des sorties qui permettent d'en étudier le fonctionnement,
2) de l'intérieur, par la mise en évidence :

. de ses caractéristiques physiques (par décomposition organique en sous-systèmes et composants),
. de ses modes d'organisation (relationnelles, hiérarchiques,…),
. de ses propriétés (autonomie, robustesse, vulnérabilité, …),
. de son comportement (dynamique d'évolution, productivité, …).

Plusieurs formes de classification en résultent. Génériques ou dédiées, elles s'appuient sur de nombreuses typologies et des caractéristiques de toutes sortes issues des champs fonctionnels *(ce que fait le système),* structurels *(qui fait quoi dans le système)*, comportementaux *(comment évolue le système)*, technologiques ou physiques *(de quoi est fait le système)* qui guideront les méthodes de modélisation.

Un système peut être complexe à cause de la nature des interactions entre les éléments qui le composent. Là encore, la complexité est décrite de plusieurs façons ; on retiendra la définition de Le Moigne [3] qui présente un tel système comme un ensemble d'éléments en relation dont les interactions font émerger de nouvelles propriétés qui ne figurent pas dans les éléments eux-mêmes.

Il faut encore faire la distinction entre système complexe et système compliqué.
S'il peut exister dans les deux cas un nombre élevé de composants, dans un système compliqué les relations entre les composants sont simples, de type arborescence [4]. De ce fait, le système est décomposable en éléments plus simples qui pourront être analysés séparément pour comprendre le système global (figure 1). Par contre, dans un système complexe, les relations entre les composants qui le constituent comportent des « boucles » ; le système est non décomposable sous peine d'altérer la compréhension.



Système compliqué Système complexe

Figure 1 : complexité d'un système

La complexité du système ne découle donc pas simplement de la quantité de ses constituants ou de la diversité de leurs interrelations ; elle correspond au nombre de configurations, d'états ou de comportements possibles du système et est la conséquence d'interactions et combinaisons et de nombreuses possibilités d'agencement ou d'évolution.

On distinguera la complexité liée à l'architecture du système de celle propre aux interférences entre composants ou avec l'environnement du système.
En analyse de système, cette double notion impose de considérer le système sur les plans structurels et temporels.

1.2 Vue structurelle ou statique

La description du système passe par sa décomposition analytique en éléments plus simples. Sa structure peut être définie de trois manières : fonctionnelle, organique et organisationnelle.
L'architecture fonctionnelle du système résulte de la décomposition de ses fonctions opérationnelles en une hiérarchie de sous fonctions.
La conception de la structure organique consiste à définir le système par une décomposition itérative des différentes hiérarchies de ses constituants jusqu'aux composants physiques élémentaires.
La définition organisationnelle du système consiste à déterminer ses modes d'organisation en intégrant les aspects hiérarchiques et relationnels.

1.3 Vue temporelle ou dynamique

La dynamique du système caractérise à la fois son fonctionnement (par exemple, la transformation des données d'entrée en données de sortie) et son évolution (adaptation du système à la mission assurée ou à l'environnement).
Cette dynamique peut exister sous trois formes temporelles : continue (variation de caractéristiques continues), discrète (à dates fixes) ou discrète (propre au système, observée à l'instant de discontinuités de fonctionnement).
Cette dynamique fait apparaître la notion de boucle de pilotage du système. Une partie des paramètres gouvernant le fonctionnement du système peut être utilisée pour son pilotage. Le pilotage est fonction de l'évolution de paramètres propres au système ou à certaines caractéristiques environnementales sur lesquelles il influe. La notion de boucle de pilotage induit trois fonctions majeures :

- la récupération d'informations (à partir de capteurs correctement positionnés),
- la mesure de l'écart entre les paramètres courants et les paramètres à atteindre (conduisant au calcul de facteurs de correction),
- la régulation du système, réalisée par injection de nouveaux paramètres déduits des facteurs de correction.

Le pilotage du système peut être effectué par anticipation ou interaction, le système est alors contrôlé en boucle ouverte par des informations prises sur ses entrées. Il peut aussi être régulé selon des principes de rétroaction, le système est alors contrôlé en boucle fermée par des informations prises sur ses sorties.

1.4 L'approche systémique et l'ingénierie système

Les notions évoquées jusqu'ici font partie des bases de l'approche systémique, méthodologie qui vise à percevoir et comprendre les systèmes dans leur complexité, leur dynamique et leur évolution.
L'analyse systémique est à la fois analytique et synthétique, détaillante et englobante ; elle conduit à la définition d'un langage unitaire de représentation des systèmes en se fondant sur leurs propriétés.

L'ingénierie système est un processus collaboratif et multidisciplinaire de résolution de problèmes. Elle prend en compte tous les domaines et disciplines impliqués dans le cycle de vie du système en considérant les différents besoins, pour développer

une solution optimisée à la fois économique, performante et satisfaisant tous les points de vue des différentes parties prenantes [5]

La croissance de complexité des systèmes impliquerait souvent de considérer le système dans une vue d'ensemble. Ceci est rarement possible ; l'ingénierie système préconise alors d'opérer un découpage conduisant à mener de front plusieurs démarches d'études (le système est décomposé en éléments) qui juxtaposent des espaces maîtrisés individuellement.

1.5 Relation entre vue structurelle et vue temporelle

L'analyse d'un système selon une vue temporelle fait séparer les phases qui jalonnent le cycle de vie du système et le processus de mise en œuvre de chaque phase. La vue produit, par exemple, met en jeu des phases séquentielles de développement, production, commercialisation, maintenance, élimination. Chaque phase est ensuite gouvernée par un processus transversal impliquant des activités génériques de spécification, définition, réalisation, suivi, capitalisation.
L'analyse complète du système requiert de considérer chaque activité du processus mis en jeu au sein de chaque phase de son cycle de vie. Cela induit les notions de système principal et de système support.
Le système est constitué :

. de ses sous-systèmes et constituants (matériels, logiciels, organisations et compétences humaines) qui forment le système principal,

. des ressources matérielles/immatérielles permettant de concevoir, produire, vérifier, exploiter, maintenir en condition opérationnelle et retirer du service chaque composant du système principal. L'ensemble de ces ressources forme le système support (ou encore système contributeur ou associé).

Cette approche de la définition du système induit une démarche d'ingénierie descendante qui s'appuie sur une décomposition itérative du système en blocs constitutifs dont elle définit les constituants, leurs interfaces et les éléments contributeurs.
L'ingénierie système peut être appliquée aussi bien au système principal qu'à ses systèmes associés : système de production réunissant les ressources destinées à la création de la valeur ajoutée, système de soutien logistique regroupant l'ensemble des produits et processus contribuant à son maintien en condition opérationnelle, système de démantèlement assurant son retrait de service. Chacun de ces systèmes a son propre cycle de vie et doit être opérationnel lorsque le système principal le nécessite.

Un exemple significatif est celui des applications d'ingénierie simultanée.
Dans ce contexte, les vues structurelles et temporelles trouvent un champ naturel d'intégration.
L'ingénierie simultanée est caractérisée par un chevauchement des étapes du cycle de vie et une prise en compte des contraintes inhérentes à chaque acteur intervenant sur le cycle de vie du produit, ceci dès le stade du développement.
Elle consiste à concevoir de façon intégrée les produits et les processus qui leur sont rattachés.
Dans le contexte d'ingénierie simultanée, un phénomène de récursivité peut être observé au niveau de la phase de développement. Celle-ci englobe la conception du

produit et son industrialisation, c'est à dire le développement du process. Considéré comme un produit, ce dernier peut être alors lui même industrialisé….

Plus généralement, l'analyse du système nécessite d'appréhender le système principal, objet du développement mais aussi ses systèmes associés. Chaque système possède sa propre structure et son propre cycle de vie. Les vues temporelles de chaque système contributeur ne sont pas découplées de celle du système principal. Des points de correspondance, instants de rencontre où se croisent les différents systèmes existent. Ils sont imposés par le système principal mais peuvent être négociés au départ en fonction des contraintes induites par le développement des systèmes associés.
L'analyse requiert par conséquent :

. une vision aussi large que possible du système et de ses systèmes associés sur le plan physique,
. une représentation claire de l'imbrication dynamique des différents processus régissant chaque système,
. une vue précise des modes d'articulation entre ces processus et des instants de coordination qui leur permettent de communiquer.

2 Mesure de performance

La performance d'un système est une caractéristique qui qualifie et/ou quantifie le résultat de l'engagement du système. Cette caractéristique est construite à partir des résultats directement produits et de la manière avec laquelle ces résultats ont été obtenus ; elle peut revêtir plusieurs formes et concerner différents traits représentatifs du système comme l'efficacité ou l'efficience.
L'efficacité désigne le fait que l'engagement du système permet d'atteindre le résultat prévu. Les mesures quantifieront le rapport entre les résultats fournis et les objectifs assignés. L'efficacité est orientée vers la qualité de la prestation fournie.
L'efficience ajoute la notion de moindre effort ou de temps minimal requis pour atteindre ce résultat. Les mesures quantifieront le rapport entre les résultats fournis et les moyens engagés. L'efficience est orientée vers la productivité.

En dehors des cas simples qui ne requièrent que l'expression de certains ratios, l'évaluation de la performance nécessite généralement de considérer les vues structurelles et temporelles du système (§1.2 et §1.3). Il faut, en effet, évaluer le système à la fois sur l'ensemble des étapes de son cycle de vie et par rapport à toutes ses composantes.

La mesure de la performance nécessite la mise en place d'indicateurs convenablement sélectionnés.
Un indicateur est une donnée quantitative qui permet de caractériser une situation évolutive, une action ou les conséquences d'une action, de façon à les évaluer et à comparer leur état à différentes dates.
Un tableau de bord définit l'ensemble des indicateurs, renseignés périodiquement et destinés au suivi de fonctionnement d'un système, de l'état d'avancement d'un programme ou d'une politique et à l'évaluation de l'efficacité de ce système, de ce programme ou de cette politique.

A partir d'un mécanisme d'évaluation et d'indicateurs positionnés à différents endroits, l'amélioration de la performance peut être schématisée suivant la représentation de la figure 2.

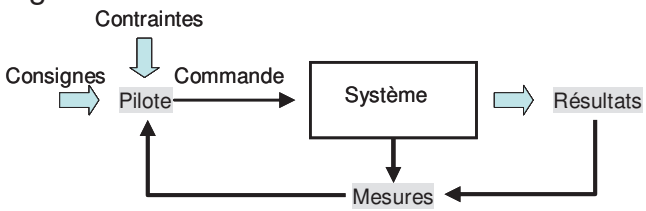


Figure 2 : mesure de performance

Ce schéma qui rappelle la boucle de pilotage décrite dans le paragraphe §1.3 illustre bien la forte corrélation entre suivi de performance et pilotage.

Le choix des indicateurs, révélateurs de « l'état » du système analysé, est essentiel pour piloter la performance de façon cohérente et rationnelle. Trop d'indicateurs peut nuire à la lisibilité du tableau de bord mais un nombre trop restreint peut conduire à occulter certaines informations utiles à une prise de décision efficace.

Bien souvent, les problèmes apparaissent aux interfaces des systèmes, zones sensibles où les responsabilités peuvent être mal définies.
Que ce soit sur le plan structurel au niveau, par exemple, des relations entre le système principal et le système de soutien, ou sur le plan temporel dans le passage, par exemple, de la phase de conception à la phase d'industrialisation, des contraintes d'adaptation ou de collaboration apparaissent et doivent être prises en compte.

2.1 Evaluation dynamique ou temps réel

L'évaluation de la performance abordée sous l'angle temporel requiert souvent un niveau de détail précis, plus fin que le découpage classique du cycle de vie précédemment énoncé.
Chaque phase de ce cycle met en jeu un ou plusieurs processus.
C'est au niveau des processus que doit être réalisée l'instrumentation permettant de procéder à la mesure de leur performance.
Chaque processus est décrit par ses objectifs et les phases qui permettent de l'atteindre.
La finalité du processus constitue un indicateur de résultat important à considérer puisque la valeur obtenue en sortie du processus ou, plutôt, l'écart de cette valeur avec l'objectif fixé témoignera directement de la performance du processus.
En rapprochant les valeurs constatées de celles visées, il devient possible de réagir aux dérives, d'apprécier les conséquences de l'application de mesures internes, de vérifier le respect de l'exécution de contrats de services externes négociés,…
L'instrumentation réfléchie des processus identifiés permet d'accéder aussi à d'autres types d'indicateurs. Ces indicateurs peuvent rester qualitatifs mais la plupart cependant sont quantitatifs : délais, coûts par activité, volumes produits,…
La confrontation entre valeurs d'indicateurs communs à plusieurs processus est une autre source d'enseignement sur l'efficacité relative des différentes activités.

On notera que cette vue dynamique concerne tous les éléments pouvant apparaître dans la nomenclature du système observé sur l'ensemble des phases de son cycle de vie. L'évaluation de l'efficacité du système concernera la quantification de la performance du système principal en phase d'utilisation comme celle du système de soutien engagé pour les opérations de maintenance par exemple.
La mesure de performance du système débouche encore sur le même constat d'imbrication entre vues structurelle et temporelle (cf §1.5).

2.2 Evaluation statique ou statistique

La mesure de performance statique permet de quantifier des caractéristiques n'intervenant pas directement en pilotage temps réel du système mais qui apparaissent dans l'établissement de stratégies d'investissement ou de changement de politique.
Cette mesure permet de décrire le système au repos ou lui assigner une signature de comportement par un dénombrement statistique basé sur une longue période d'observation.
Les outils de mesure de la performance du système sont ici :

. des indicateurs statiques, liés aux aspects dimensionnels (associés à la taille du système) et économiques, caractérisant l'immobilisation financière induite par la dimension du système,

. des indicateurs statistiques, liés aux aspects productifs (rendement moyen, volumes moyens produits,…), à la qualité (nombre moyen de rebuts, d'accidents du travail,…), à la composante humaine (taux moyen d'absentéisme, d'arrêt maladie, nombre de jours de grève,…) et, toujours, aux aspects économiques (valeur ajoutée moyenne, coûts moyens de production, chiffre d'affaire,…).

2.3 Position de la sûreté de fonctionnement

La sûreté de fonctionnement occupe une place forte dans la réalisation de performance du système. Les modes de marche du système : marche normale (nominale), dégradée,… vont conditionner cette performance ; la gestion efficace de ces modes va permettre de réaliser la performance requise.
Si nous résumons les états de fonctionnement du système par la partition entre deux états de bon fonctionnement et d'interruption de service de la figure 3 (états E1 et E2), les mesures de sûreté de fonctionnement peuvent guider les mesures de la performance du système.

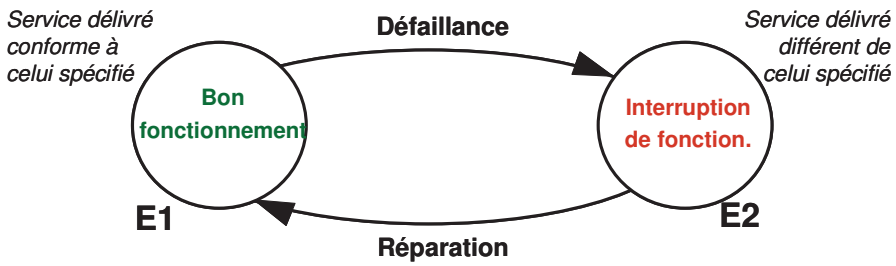


Figure 3 : états du système

Le lecteur peut trouver une présentation détaillée de ces mesures de sûreté de fonctionnement dans de nombreux ouvrages et articles dédiés comme, par exemple, les dossiers des Techniques de l'Ingénieur [6] [7]. Nous ne rappelons ici que certaines mesures courantes :

. la fiabilité qui caractérise le bon fonctionnement continu du système :
$R(t)$ = Probabilité $\{Z(t) \in E1 \mid Z(t) \in E1, 0 \leq t < t\}$
ou encore $R(t)$ = Probabilité $\{Z(t) \in E1, 0 \leq t < t\}$, avec $Z(t)$ fonction état du système :
$Z(t) = Ei$ si le système est dans l'état Ei à la date t,
qui peut donner, par exemple, le taux de défaillance, inverse du MTTF (Mean Time To Failure) temps moyen jusqu'à la première défaillance,

. la disponibilité qui traduit l'aptitude du système à exécuter les tâches qui lui sont confiées lorsqu'il est sollicité
$A(t)$ = Probabilité $\{Z(t) \in E1 \mid Z(t) \in E1UE2, 0 \leq t < t\}$,

. la maintenabilité qui traduit l'aptitude à la localisation et à la réparation des éléments défaillants
$M(t)$ = Probabilité $\{Z(t) \in E1 \mid Z(t) \in E2, 0 \leq t < t\}$
conduisant au MTTR (Mean Time To Repair : temps moyen de réparation ou de retour du système dans l'état de bon fonctionnement).

Il est très facile d'interpréter ces métriques et de les corréler directement à des indicateurs de performance du système.

Une partition plus fine des états du système en fonction, par exemple, de plusieurs niveaux de marche dégradée ou de différentes formes d'interruption de service, permettra d'établir des informations plus précises sur la performance du système.

Il faut juste rappeler ici l'étroite dépendance entre les caractéristiques de sûreté de fonctionnement et de performance technique et les caractéristiques de coûts directs/ indirects (conception, développement, exploitation,…) associés au système ; ces trois « dimensions » sont toujours très fortement corrélées (figure 4).

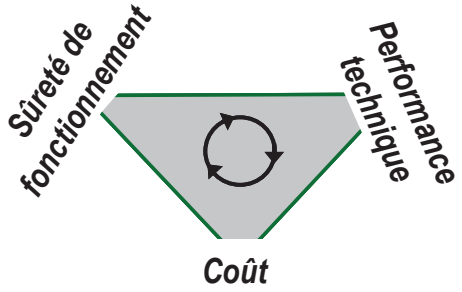


Figure 4

L'exploitation d'une structure de coût (bénéfices, pénalités,…) associée aux temps d'occupation d'états ou aux événements déclencheurs de changement d'états permettra de caractériser cette performance économique.

3 Méthodes d'analyse technique et fonctionnelle

Il a été introduit dans le paragraphe précédent les modes d'évaluation de la performance, passage obligatoire en vue de procéder à l'analyse de l'efficacité d'un système. Ces notions mettent clairement en évidence un besoin de méthodes d'analyse et de modélisation du système sous l'angle technique et fonctionnel, formant une étape essentielle dans la démarche d'évaluation

Cette première étape peut s'appuyer sur des méthodes d'analyse éprouvées dont plusieurs sont couramment utilisées en sûreté de fonctionnement.

Les principaux outils, méthodes et techniques exploitables dans un contexte d'analyse de systèmes sont résumés ci-après.
Cet état est limité aux outils d'usage industriel courant et constitue, par conséquent, une collection non exhaustive. De plus, n'ont été inventoriés que les principaux représentants de chaque type d'outils, en écartant les variantes d'outils et outils dérivés.

Le premier niveau d'analyse porte sur l'acquisition des informations et le recueil des connaissances pour construire une première base de connaissances sur lesquelles porteront la modélisation et l'analyse proprement dite du système. Ces méthodes peuvent être :
. informelles, c'est-à-dire qu'il n'existe aucune sémantique ou syntaxe guidant l'élaboration de l'information,
. semi-formelles, s'appuyant sur une amorce de syntaxe (arbres...) et/ou de sémantique (questionnaires guidés...).

On trouvera à ce niveau une large panoplie d'outils de type :
. interviews,
. questionnaires et "checks-lists",
. méthodes de classification (catalogues),
. grilles d'évaluation.

Il est à noter que plusieurs méthodes de recueil de connaissances (KADS (Knowledge Acquisition and Design Structuring), KOD (Knowledge Oriented Design),… [8]) destinées à transformer les connaissances non formalisées (connaissances tacites) en connaissances explicites s'appuient sur des principes comparables.

L'étape suivante est généralement celle de (première) modélisation.
Le système global pourra être considéré, selon la méthode retenue, sous forme d'activité, de données ou de processus (figure 5).

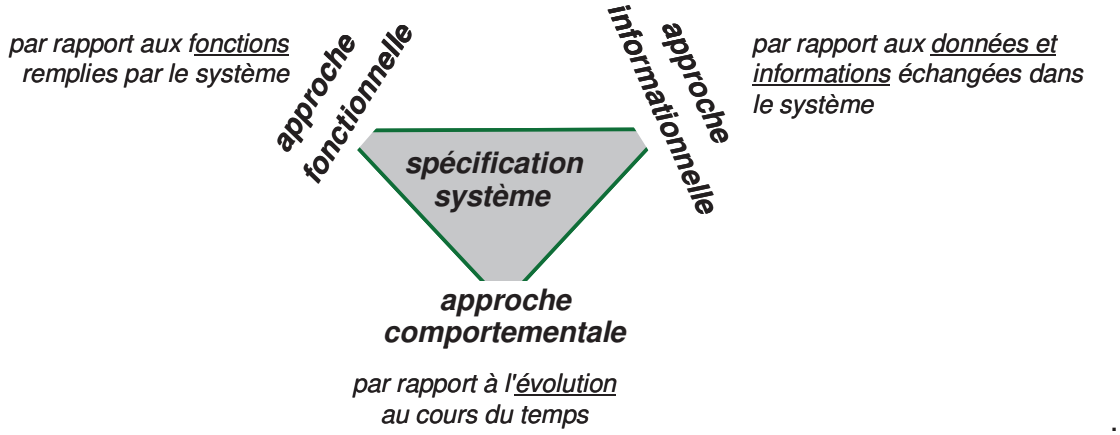


Figure 5 : "description" d'un système

Les méthodes d'analyse peuvent être distinguées suivant trois types présentés ci-après.

Les méthodes fonctionnelles.
Ces méthodes permettent l'identification des fonctions à assurer. Elles sont basées sur une approche structurée de manière hiérarchique, descendante et modulaire. A partir de raffinements successifs, ces méthodes qui s'appuient très souvent sur un formalisme graphique débouchent sur des spécifications.
Chaque niveau peut ensuite être décomposé en respectant les entrées-sorties du niveau supérieur. La décomposition se poursuit jusqu'à l'obtention du niveau de détail jugé suffisant pour l'analyse.
Parmi les méthodes d'analyse figurant dans cette catégorie on peut citer les méthodes :

. APTE (Application des Principes d'Entreprise),
. ASA (Analyse Structurée d'Automate),
. FAST (Function Analysis System Technique),
. FBS (Function Breakdown Structure), PBS (Product Breakdown Structure) et WBS (Work Breakdown Structure),
. SADT (Structured Analysis and Design Technique), SA (Structured Analysis) et SART (Structured Analysis and Real Time).

Ces méthodes sont décrites en détail dans de nombreux articles spécifiques (voir [9] par exemple) et ne seront pas développées plus avant ici. Notons seulement que certaines d'entre-elles ne sont pas seulement appliquées à l'identification des fonctions réalisées (ou à réaliser) par le système mais qu'elle sont engagées dans le processus même de conception du système.

D'autres outils, basés sur les mêmes principes, sont disponibles pour l'analyse de systèmes particuliers. Citons, par exemple :

. l'approche Merise [10] pour le traitement des systèmes d'information, basée sur la séparation des données et des traitements à effectuer en plusieurs modèles conceptuels et physiques,
. la méthode Grai [11] pour celui des systèmes décisionnels, s'appuyant sur un modèle conceptuel élaboré selon différents points de vue à partir des théories sur les systèmes, les systèmes hiérarchisés et les systèmes d'organisation.

Enfin, d'autres approches, tel UML (Unified Modeling Language), permettent aussi une représentation des situations ou des systèmes à base d'objets ou d'agents. UML, par exemple, largement utilisé dans divers domaines même s'il est issu du développement informatique, est un des standards de modélisation qui permet de spécifier, visualiser, construire et documenter tout type de processus et/ou d'organisation suivant différentes vues (neuf types de diagrammes) sans formalisme strict [12] [13].

Les méthodes statistiques.
Basées sur l'observation d'événements expérimentaux, ces méthodes visent à établir, par des techniques mathématiques, des hypothèses qui permettront de prédire des événements dans des situations analogues. Les méthodes statistiques pures utilisées pour décrire un échantillon de données peuvent être classées en méthodes de régression, d'analyse de la variance, d'analyse multivariée.
Divers supports de type « analyse des données statistiques », souvent corrélés aux méthodes et outils de gestion de la qualité, sont accessibles à ce niveau.

Des méthodes plus élaborées permettent l'établissement d'indicateurs spécifiques et sont bien adaptés à l'établissement d'éléments de tableaux de bord. On peut citer en particulier des méthodes comme :
. Diagramme de Pareto et méthode ABC,
. Lois statistiques (beta, normal, poisson, weibull, théorème centrale limite…).

Une présentation de ces méthodes peut être trouvée dans les articles [14] et [15].

Rappelons encore, parmi les outils de traitement, ceux fondés sur l'algèbre booléenne et les opérateurs logiques qui permettent une agrégation de l'information ou, ceux qui s'appuient sur la théorie stochastique pour :
- établir les probabilités servant aux calculs de base : l'Analyse Probabiliste,
- ou traiter une information hétérogène (historique et prévisions) : la théorie de Bayes et les réseaux Bayesiens,
que nous retrouverons dans le paragraphe 5 parmi les outils d'évaluation de la sûreté de fonctionnement.

Enfin, en relation avec les méthodes de recueil de connaissances, on peut citer l'approche de la méthode DELPHI [16] qui associe les analyses de groupes d'experts dans une forme interactive de convergence (débat contrôlé) pour aboutir à un consensus .

Les méthodes de simulation.
Ces méthodes sont utilisées lorsque le nombre de données à traiter rend le calcul analytique complexe. Elles permettent de représenter virtuellement le comportement du système soumis à des contraintes choisies dans un environnement donné.
Ces méthodes peuvent être génériques comme celles basées sur les systèmes à événements discrets utilisées dans le cadre de la simulation de flux avec des outils de type Réseau de Petri [17] ; elles peuvent aussi être propres à des disciplines comme, par exemple, la méthode des différences finies, très utilisée dans le domaine de la conception mécanique.

Citons, parmi les méthodes de simulation dynamique, la simulation de Monte Carlo qui prend en compte la dynamique d'événements et permet d'établir des données statistiques, méthode que nous retrouverons, elle aussi, en évaluation de sûreté de fonctionnement.

Les outils et méthodes cités précédemment permettent l'analyse du système considéré dans des conditions nominales de fonctionnement. La qualité des résultats dépend des hypothèses faites dans l'approche de modélisation.
Globalement, ces méthodes d'analyse ne prennent en compte que les paramètres connus ou envisagés pour décrire le système et son évolution ; elles n'intègrent pas la notion d'incertitude et le caractère aléatoire liés à l'apparition de phénomènes non maîtrisés par le concepteur ou l'utilisateur. Seules, les méthodes statistiques se référant au passé du système abordent cet aspect mais elles restent limitées à ce passé sans considération sur ce qui pourrait arriver mais qui ne s'est pas produit.

La prise en compte des paramètres incertains (données, hypothèses,…) et, plus largement la considération des modes anormaux sont nécessaires à une description plus fidèle du système et à une évaluation réaliste des performances.
Les méthodologies et démarches de calcul à engager porteront sur le traitement de problèmes stochastiques, c'est-à-dire de problèmes dans lesquels le hasard entre en jeu.

L'incertitude pourra être directement intégrée à ces méthodes par la connaissance de sa forme de distribution. C'est l'objet du paragraphe suivant.

4 Gestion de l'incertitude

L'analyse des systèmes trouve son origine dans le caractère incertain des paramètres mis en jeu. Cette incertitude peut être appréhendée sous deux formes principales par application des techniques probabilistes ou possibilistes [18].

4.1 La vue probabiliste

L'analyse probabiliste vise à évaluer l'occurrence potentielle d'un événement aléatoire sur une échelle linéaire comprise entre 0 (événement impossible) et 1 (événement certain). Deux approches sont possibles :
- l'approche fréquentiste (ou inférentielle) correspondant au dénombrement des cas favorables sur le nombre de cas possibles [15],
- l'approche bayesienne, issue du théorème de Bayes, permettant de calculer des probabilités a posteriori et utilisant les connaissances a priori du phénomène aléatoire dans un modèle statistique.
On utilisera l'approche fréquentiste si l'on dispose d'un grand nombre de données jugées représentatives ; on préférera la deuxième lorsque les données sont rares ou difficiles à collecter.

L'analyse probabiliste utilise la notion de variable aléatoire, continue ou discrète, obéissant à une loi de probabilité.

La fonction de probabilité (ou distribution de probabilité) assigne une probabilité à chaque valeur prise par la variable aléatoire. On parlera de densité de probabilité si on se trouve dans le cas continu, de fréquence dans le cas discret.
Le cumul des valeurs prises par la variable aléatoire peut être représenté pour chacune de ces valeurs par une fonction de distribution. Cette fonction sera déduite d'un calcul intégral de la fonction de densité pour une variable aléatoire continue, d'une somme des fréquences dans le cas discret.
Le complément à 1 de la fonction de distribution est appelé fonction de survie ou fonction de fiabilité.
Différentes lois de probabilités classiques peuvent être utilisées pour modéliser (simuler) l'événement aléatoire étudié. Le choix de la loi représentative est fonction du caractère continu ou discret de la variable aléatoire, des données disponibles sur l'événement, de la facilité d'adaptation de la loi,…

On qualifie de problème d'ajustement ce problème de choix, dans une famille de lois de probabilité, de celle qui correspond le mieux à l'ensemble des données (échantillon d'observation) dont on dispose.
Lorsque la famille dépend d'un ou plusieurs paramètres réels inconnus, le problème est de déterminer la valeur du paramètre la mieux adaptée aux données (problème d'estimation paramétrique). Plusieurs méthodes permettent cette estimation des paramètres : la méthode des moments, la méthode du maximum de vraisemblance, la méthode des moindres carrés,…
Les méthodes non paramétriques sont utilisées lorsque les hypothèses du modèle paramétrique classique ne sont pas vérifiées ou que le nombre de données n'est pas suffisant ou, encore, lorsque des valeurs aberrantes sont présentes dans l'échantillon. Aucune hypothèse n'est alors faite sur la loi de probabilité ; la loi est approchée par une fonction mathématique construite à partir des seules valeurs de l'échantillon. On peut citer parmi les méthodes d'estimation non paramétriques les méthodes de Wayne Nelson, de Kaplan Meier, de Johnson…[19].

Les méthodes d'ajustement paramétriques ou non paramétriques permettent d'identifier une loi plus ou moins représentative de l'échantillon initial. La différence entre l'observation et ce modèle peut conduire à des résultats erronés si la loi choisie n'est pas représentative du phénomène étudié.
Il est important de s'assurer que la distribution envisagée correspond bien aux données observées. Un certain nombre de techniques, parmi lesquelles figurent les tests d'adéquation, ont été développées pour vérifier cette compatibilité : tests du khi-deux, de Shapiro Wilk, de Kolmogorov Smirnov ou de Fisher et Student [19].

Une limite à l'approche probabiliste est de ne pas représenter la différence entre deux états de connaissance se distinguant uniquement par une différence de confiance dans les informations disponibles. Dans ces situations, l'approche possibiliste et ses outils de représentation pourront être préférés pour représenter l'ignorance et prendre en compte la pertinence d'une information incertaine.

4.2 La vue possibiliste

Dans cette démarche, les variables utilisées sont des variables floues.
La notion de variable floue est apparue en 1965 à Berkeley avec la théorie des sous-ensembles flous puis en 1978 avec la théorie des possibilités. Ces deux théories

constituent aujourd'hui la logique floue. L'ouvrage [20], référence dans ce domaine, peut être utilisé pour éclairer ces aspects.

Les champs d'application de la logique floue sont multiples : aide à la décision et au diagnostic, reconnaissance de forme, agrégation multicritère et optimisation, commande floue de systèmes. Plus généralement, la logique floue sera utilisée dans les situations mettant en évidence le caractère incertain ou imprécis de grandeurs comme, par exemple :

. une connaissance numérique mal connue à cause d'insuffisances des instruments de mesure (erreurs de mesure…),

. une connaissance vague (perception symbolique, catégories aux limites mal définies),

. une connaissance incomplète (ou l'absence de connaissance),

. une connaissance implicite non exprimée, une connaissance non dénombrable,

ou encore :

. l'ignorance partielle sur la validité d'une connaissance,

. la fiabilité relative du dispositif de perception d'informations,

. la difficulté d'obtention ou de vérification de la connaissance.

Le principe de fonctionnement de l'approche floue suit trois étapes distinctes (figure 6).

1- La quantification floue : cette étape permet d'associer à chaque variable d'entrée son degré d'appartenance aux états du système.

Des fonctions d'appartenance sont déterminées à partir d'une partition en classes de l'ensemble des valeurs que peuvent prendre les variables. Ces fonctions sont de forme triangulaire, rectangulaire ou trapézoïdale pour les plus courantes mais elles peuvent être de forme quelconque (figure 6). Ces fonctions d'appartenance délimitent des ensembles flous.

Comme pour la théorie classique des ensembles, on peut définir la réunion, l'intersection, le complément d'ensembles flous.

2- L'inférence : cette étape consiste à réaliser une opération logique par laquelle on admet une proposition en vertu de sa liaison avec d'autres propositions tenues pour vraies. Il s'agit d'établir des règles du type si <X est A> et <Y est B>, alors <Z est C>. Le contenu des deux premières parenthèses est qualifié de prémisses, le contenu de la troisième représente l'implication. L'élément linguistique de liaison entre les deux premières prémisses s'appelle la conjonction.

La conclusion d'une règle floue est l'appartenance d'une variable floue de sortie à une classe floue de sortie. Cette appartenance dépend de la classe floue de sortie considérée, du degré de validité de la prémisse et de la méthode d'implication choisie.

3- La défuzzification : cette étape consiste à associer à un ensemble flou un nombre interprétable par l'utilisateur ou l'interface de commande. A ce niveau les prémisses sont combinées et les règles sont agrégées pour fournir une valeur de sortie en réponse à une valeur d'entrée.

Deux méthodes de défuzzification sont classiquement utilisées : la méthode du centre de gravité qui consiste à considérer l'abscisse du centre de gravité de la surface sous la courbe résultat et la méthode moyenne des maximums qui considère la moyenne des valeurs de sorties les plus vraisemblables.

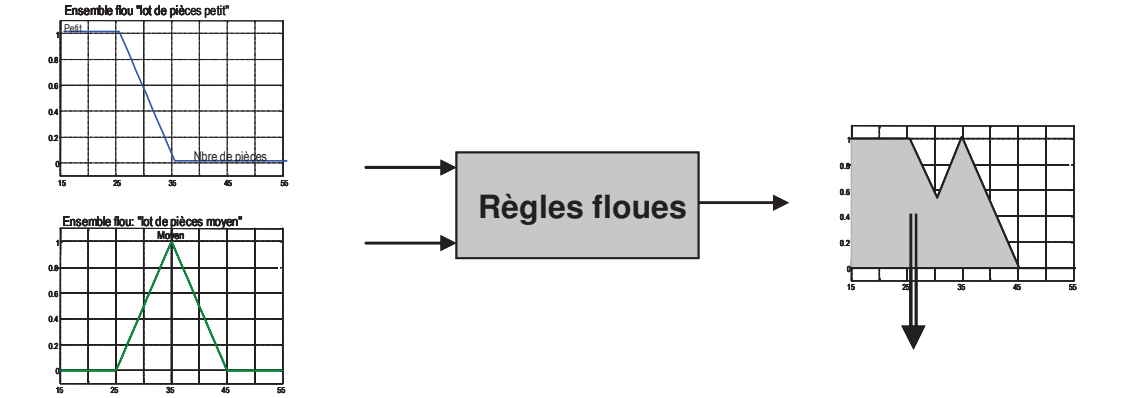


Figure 6 – approche possibiliste

5 Méthodes d'évaluation de la sûreté de fonctionnement

5.1 La sûreté de fonctionnement dans l'évaluation des performances

Les caractéristiques de sûreté de fonctionnement ou le comportement FMDS (Fiabilité-Maintenabilité-Disponibilité-Sécurité) du système influent d'une façon majeure sur ses performances opérationnelles et entrent, de fait, dans l'évaluation de cette performance (paragraphe 2.3).

Directement, par l'expression, par exemple, de la disponibilité opérationnelle du système ou indirectement, par le calcul, par exemple, du coût total de possession, l'évaluation de sûreté de fonctionnement est étroitement couplée aux processus décisionnels engagés en conception et conduite des systèmes.

L'intégration de la notion de probabilité dans les théories et méthodes de dimensionnement n'est pas suffisante pour caractériser l'ensemble des risques.

La démarche d'évaluation dont on a donné un aperçu dans le paragraphe 2.3 est plus complexe.

Cette démarche s'appuie évidemment sur la connaissance des modes de fonctionnement normal du système, résultat d'une première étape d'analyse fonctionnelle et de comportement qui engagera les outils tels que ceux présentés dans le paragraphe 3.

Elle nécessite ensuite la connaissance des modes de dysfonctionnement avec l'identification des phénomènes intrinsèques et extrinsèques au système, susceptibles d'affecter son fonctionnement.

Une structuration de cette démarche générale d'analyse, orientée autour des axes fonctionnel et dysfonctionnel, a été proposée dans le cadre d'une méthodologie intitulée Maintenance Centrée sur la Fiabilité (aussi appelée Optimisation de la

Maintenance par la Fiabilité). Le principe de cette démarche d'analyse est représenté sur la figure 7.

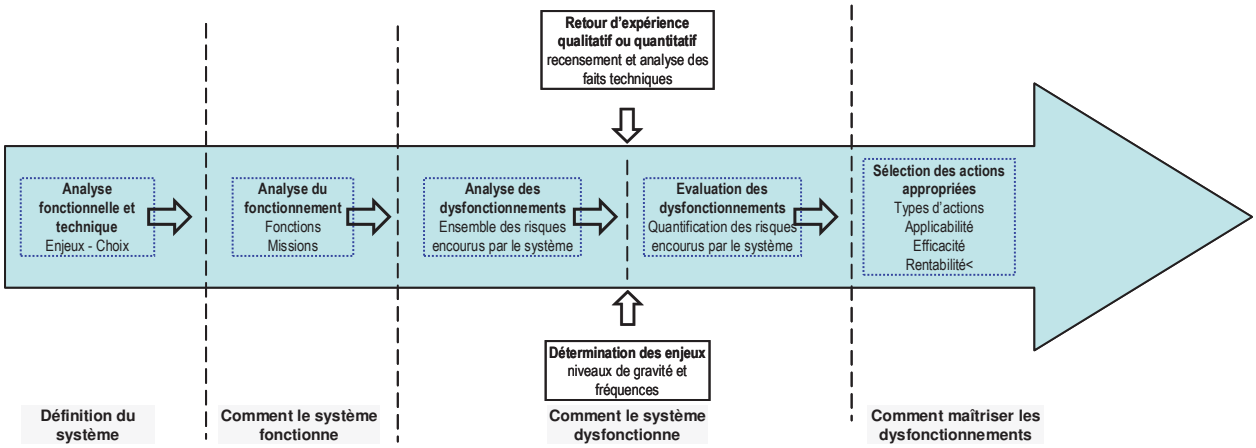


Figure 7 : démarche d'analyse de sûreté de fonctionnement

On retrouve sur ce schéma un processus désormais classique en maîtrise des risques.

Le risque est une évaluation du danger (i.e. d'une situation qui comporte un certain potentiel à causer des dommages aux biens et aux personnes).

Le risque implique éventualité et hasard, possibilité ou probabilité, certitude ou incertitude. Il est défini dans la norme ISO/IEC Guide 73 [21] comme « la combinaison de la probabilité d'un événement et des conséquences de celui-ci ». Paradoxalement, la prédiction du risque est rendue possible par ce caractère incertain : l'aléa obéit à des règles que le recueil statistique et le calcul probabiliste permettent de saisir. La notion de risque apparaît donc comme un réducteur d'incertitude, caractéristique d'une l'activité prospective qui vise à maîtriser l'avenir.

5.2 La cyndinique dans l'évaluation des performances

Outre la sûreté de fonctionnement, il existe une autre approche pour appréhender le risque afin de l'éliminer ou d'en diminuer les conséquences néfastes : la cyndinique.

La cyndinique considère le risque sous un angle conceptuel et global. Elle permet de clarifier des aspects sémantiques et propose des modèles simples d'appréhension de certains phénomènes, le plus souvent dans des domaines techniques.

Basée sur une approche « transdisciplinaire », la cyndinique inclut toutes les sciences de l'ingénieur et les sciences humaines humaines. Elle vise une très large gamme de risques : catastrophes naturelles, risques écologiques, technologiques ou sanitaires, délinquance, accidents de la route, sportifs ou domestiques,...

Cette approche est à l'origine d'une méthodologie : la Méthode Organisée et Systémique d'Analyse de Risques (MOSAR) et d'un modèle conceptuel : le Modèle d'Analyse des Dysfonctionnements Systèmes (MADS) [22]. Organisée en dix étapes, MOSAR permet une double approche du système : d'abord macroscopique avec

l'analyse des risques principaux puis microscopique avec celle des risques de fonctionnement. De même, le modèle MADS mis en œuvre pour caractériser « l'univers du danger » distingue le(s) système(s) source(s) du danger et le(s) système(s) cible(s) de celui-ci.

Les cyndiniciens ont mené des réflexions intéressantes sur les mécanismes génériques de genèse des dangers. Une grande partie des outils et des méthodes utilisés sont toutefois issus de la Sûreté de Fonctionnement que nous considérons dans ce chapitre.

5.3 Les outils adaptés de la sûreté de fonctionnement dans l'évaluation des performances

La sûreté de fonctionnement regroupe un ensemble de techniques mises en œuvre pour identifier, analyser, gérer et, le cas échéant, réduire les risques liés aux systèmes industriels. Dans [23], Villemeur définit la sûreté de fonctionnement comme « la science des défaillances ». La Sûreté de Fonctionnement est en effet une véritable discipline qui s'appuie sur un support méthodologique applicable aux systèmes technologiques tout au long de leur cycle de vie : expression du besoin, conception, industrialisation, production, utilisation, diffusion, maintenance, voire même retrait de service.

Ces activités bénéficient du support de méthodologies rigoureuses et d'outils pratiques et puissants. Les méthodes de la sûreté de fonctionnement ont toutes au moins trois points communs, qui peuvent être résumés en trois types d'action :

- identifier les processus pouvant affecter la fiabilité, la maintenabilité, la disponibilité ou la sécurité,
- modéliser ces différents processus afin de faciliter la compréhension des mécanismes mis en jeu,
- valoriser les résultats des analyses en utilisant les modèles obtenus pour apprécier le niveau de sûreté de fonctionnement du système étudié, en relever les éventuelles insuffisances par rapport aux objectifs de performances poursuivis, en hiérarchiser les points forts et les points faibles.

De nombreux travaux proposent un inventaire de ces méthodes. On peut citer, entre autres présentations [23], [24], [25], [26], [27],…. Plusieurs dossiers des Techniques de l'Ingénieur ont été consacrés à la sûreté de fonctionnement [28] [29] [30].

Trois modes de classification sont couramment rencontrés :

- Approches qualitatives/quantitatives
  . Approches qualitatives/quantitatives
  les résultats renseignent sur les caractéristiques du système : points faibles du système, fausses redondances, influence d'un élément donné sur la fiabilité du système, repérage des chemins critiques, test (pour les chemins critiques) des méthodes d'élimination,…
  . Approches quantitatives
  les résultats sont ceux de calcul de fiabilité, disponibilité,… exemple : probabilité d'occurrence d'une combinaison d'événements ou de la racine d'un arbre.

- Approches inductives/déductives

. Approches inductives

basées sur une démarche descendante, elles considèrent un événement initiateur (défaillance technique, dysfonctionnement organisationnel, …) dont elles cherchent à caractériser les conséquences sur le système et son environnement.

. Approches déductives

basées sur une démarche ascendante, elles considèrent un événement redouté (arrêt du système, anomalie de fonctionnement, …) dont elles cherchent à expliquer les causes, le plus souvent sous forme de séquences d'événements.

- Approches statiques/dynamiques

. Approches statiques

elles permettent d'analyser le système d'un point de vue structurel sans tenir compte des évolutions au cours du temps ; elles s'appuient sur un modèle mathématique booléen du système qui fournira, par exemple, les combinaisons de défaillances entraînant la perte du système mais sans représenter les interrelations temporelles qui l'affectent.

. Approches dynamiques

les méthodes dynamiques permettent la prise en compte des aspects comportemental et temporel.

Les données d'entrée de ces méthodes sont de deux ordres :

- connaissance du système résultant généralement d'une étude fonctionnelle (cf. outils donnés dans le paragraphe 3) ou de la connaissance d'experts,

- données de nature événementielle, sous forme brute : états, historiques,... ou sous forme de modèle statistique : lois mathématiques décrivant les fonctions de distribution des événements.

Les résultats établis en sortie sont :

- des modèles de comportement du système (vis-à-vis des défaillances, réparations,…, sollicitations, service,…)

. modèles de sûreté de fonctionnement

. modèles mixtes sûreté de fonctionnement/performance,…

- des grandeurs établies à partir des modèles et pouvant revêtir différentes formes :

. probabilités d'états ou d'occurrence d'événements,

. quantificateurs FMDS : fiabilité, maintenabilité, disponibilité, sécurité,…, MTBF,…,

. métriques évoluées de performance et de coût,

- des éléments de stratégies d'actions :

. de maintenance : fréquence d'entretien,…,

. de gestion de risques : évitement,…

par association des outils de sûreté de fonctionnement à des outils décisionnels.

Des méthodes de base destinées à bien comprendre le fonctionnement du système sont souvent utilisées dans un premier temps ; elles permettent une analyse globale du système et conduisent à une première identification des risques (figure 8).

Les méthodes engagées pour les aspects fonctionnels et techniques du système sont celles énoncées dans le paragraphe 3. Elles permettent de décrire et caractériser le système dans ses modes de fonctionnement normal.
Ces méthodes de base sont presque toutes de nature inductive et n'engagent pas de modèle formel ou mathématique en aval. Plusieurs, cependant, proposent un formalisme pratique (certaines méthodes d'analyse structurée, l'approche objet,...) dont l'emploi peut être étendu au delà des spécifications de départ.

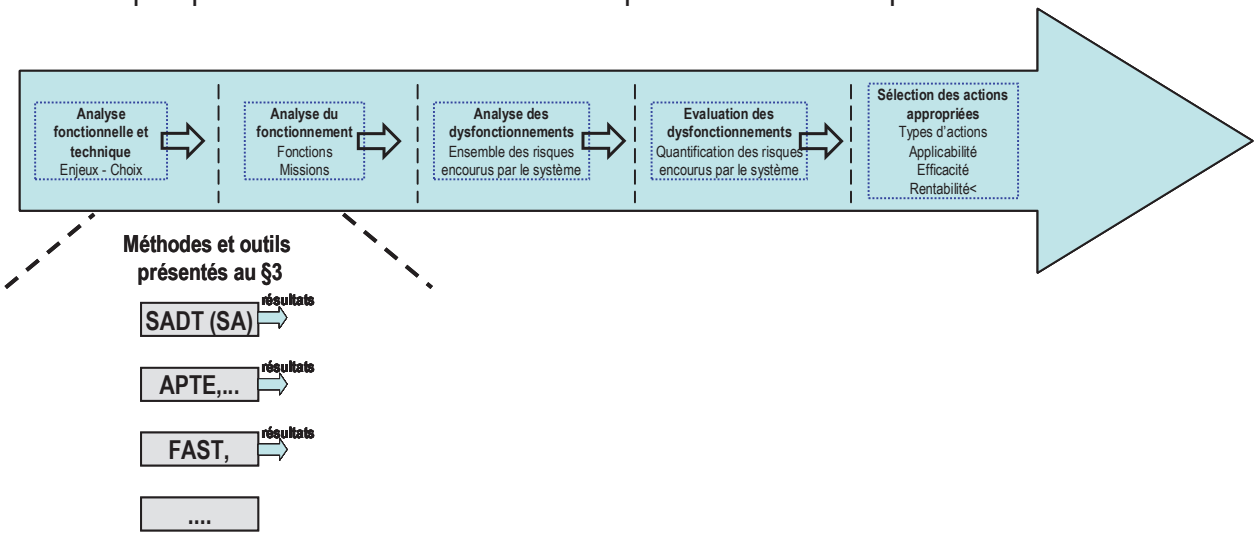


Figure 8 - méthodes de base

Les méthodes utilisées pour l'analyse dysfonctionnelle, davantage spécialisées, se présentent également sous des aspects divers : formes tabulaires, arborescence, réseaux, graphes,... Elles permettent une analyse qualitative des phénomènes et situations examinées, analyse qui peut être souvent étendue à des aspects quantitatifs (figure 9).

Pour ces méthodes, les modèles de données et/ou de connaissance du système accessibles en entrée revêtent toutes les formes possibles : listes, formes tabulaires, expressions analytiques (résultant de traitement statistique),…
L'engagement des méthodes conduit généralement à une forme structurée des sorties.
Les principales méthodes considérées à ce niveau sont évoquées ci-après.

AMDEC
L'Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité, extension de l'AMDE (Analyse des Modes de Défaillances et de leurs Effets), est une méthode ascendante qui, à partir d'un recensement des défaillances susceptibles d'affecter un système et de leur criticité, permet d'évaluer les effets de chaque mode de défaillance des composants du système sur les différentes fonctions de celui-ci et d'identifier ceux influant les caractéristiques FMDS du système [31]. Il est mis en évidence pour chaque mode de défaillance : les causes, les effets, les moyens de détection, ceux de compensation,...

statique	✓	inductif	✓	qualitatif	✓
dynamique		déductif		quantitatif	✓

Plusieurs autres méthodes s'appuient, de manière analogue à l'AMDEC, sur une représentation tabulaire de la connaissance. Citons les méthodes d'Analyse Préliminaire des Dangers (APD), des Risques (APR), d'Analyse Opératoire des Dangers (HAZOP (Hazard and Operability)), toutes essentiellement qualitatives.

L'arbre de fautes (AF)
L'AF (ou encore la Méthode de l'Arbre des Causes (MACA), la Méthode de l'Arbre de Défaillances (MAD)) est une méthode graphique descendante qui permet de combiner des éléments par leurs états, des événements, des fonctions d'un système [32]. La méthode autorise plusieurs niveaux d'abstraction, La démarche consiste à décrire graphiquement au moyen d'une structure arborescente un enchaînement causal depuis un événement indésirable unique et rechercher, le plus en amont possible, les causes de cet évènement. L'arbre est formé de niveaux successifs tels que chaque évènement résulte d'évènements des niveaux inférieurs liés par certaines relations logiques. La décomposition est arrêtée lorsqu'elle met en oeuvre des évènements de base, non décomposables, indépendants et pouvant être caractérisés par des taux d'occurrence.

statique	✓	inductif		qualitatif	✓
dynamique		déductif	✓	quantitatif	✓

La méthode de l'arbre des conséquences (MAQS) qui distingue les situations de succès et d'échec consécutives à un événement indésirable s'appuie sur les mêmes principes d'analyse tout comme la méthode des arbres d'événements (MAE).
Bien sûr, la même forme d'approche peut être appliquée pour analyser les conditions de réussite de la mission ; la Méthode du Diagramme de succès (MDS) est basée sur cette approche.
Plusieurs autres méthodes exploitent cette représentation arborescente des situations. Citons quelques outils particuliers : le diagramme d'Ishikawa (ou causes-effet) qui permet la recherche systématique des causes possibles d'un effet donné organisées en niveaux d'antériorité et classées en cinq catégories, les graphes d'éventualité, les graphes de décision,...

. Le diagramme de fiabilité (DF)
Le diagramme de fiabilité permet de déterminer la fiabilité globale d'un système et présente l'intérêt d'offrir une modélisation quasi directe de sa vue fonctionnelle. La représentation consiste en la juxtaposition série, parallèle ou mixte de blocs associés aux entités de base du système traduisant les conditions d'accomplissement du service à fournir par le système. L'association d'une expression booléenne à la structure topologique permet d'accéder à des résultats quantitatifs.

statique	✓	inductif		qualitatif	✓
dynamique		déductif	✓	quantitatif	✓

D'autres outils, proches de ceux décrits ci-dessus, peuvent être utilisés.

Parmi ceux-ci, il faut distinguer la méthode du Diagramme Cause-Conséquences ou cause-effet (MDCC) qui exploite de manière combinée les principes de l'analyse déductive de la méthode MAD et ceux de l'analyse inductive de MACS.

Les principaux résultats sont donnés sous forme :

- de répertoires des situations dangereuses et des modes de défaillance,
- de séquences d'événements inacceptables ou d'ensembles d'éléments (coupes) dont la défaillance entraîne celle du système.

L'analyse qualitative de ces résultats, notamment celle des coupes minimales [32], permet d'établir :

. les points faibles du système,
. les fausses redondances,
. l'influence d'un élément donné sur la fiabilité du système**,**
. les chemins critiques,
. les effets, pour les chemins critiques, des méthodes d'élimination

Lorsque les méthodes permettent une analyse quantitative, les traitements consistent principalement à établir les probabilités d'occurrence des coupes minimales à partir de celles des événements élémentaires et, par suite, celle des "racines" des modèles, autorisant ensuite les calculs de fiabilité.
Ces traitements et les modèles qui les sous-tendent ont, pour la plupart, une limitation d'application liée à l'obligation d'indépendance stochastique entre les événements considérés. Certaines méthodes analytiques permettront une évaluation quantitative hors de cette hypothèse.

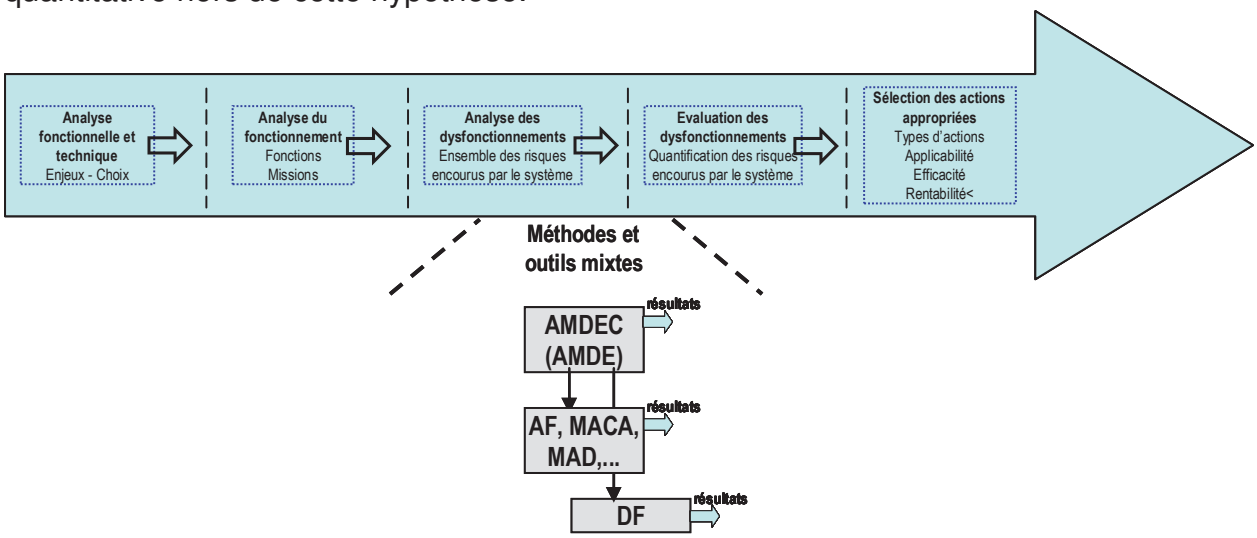


Figure 9 – Analyse des dysfonctionnements

Les méthodes d'analyse quantitative sont maintenant abordées.
Ces méthodes concernent le traitement de problèmes stochastiques, c'est-à-dire de problèmes dans lesquels le hasard entre en jeu. Il s'agit le plus souvent de méthodes dynamiques.
Plusieurs formes successives ou alternatives de traitement sont possibles suivant les objectifs, engageant plusieurs caractéristiques d'outils (figure 13).

. Outils de calculs probabilistes (CP)

Il s'agit d'un ensemble d'outils utilisant les différents théorèmes généraux du calcul des probabilités (totales, composées, conditionnelles,…) [33] [34] ; ces calculs permettent d'établir l'occurrence d'événements et les moyens de caractérisation des variables aléatoires pour simuler des lois de processus stochastiques.

statique	✓	inductif		qualitatif	
dynamique	✓	déductif	✓	quantitatif	✓

Les résultats sont du type probabilités d'événements, lois de comportement,… Ces outils prolongent bien la plupart des méthodes précédemment évoquées.

. Réseaux bayésiens (RB)
Basé sur les probabilités conditionnelles et dérivé du théorème de Bayes, cet outil permet d'établir une prévision du futur à partir du passé [35].
Il utilise deux composantes :

. un graphe causal orienté et acyclique ; les nœuds représentent les variables d'intérêt du domaine, les arcs les relations de dépendance entre ces variables (le graphe est une représentation qualitative de la connaissance),

. un ensemble de distributions locales de probabilités qui constituent les paramètres du réseau ; chaque nœud comporte une table de probabilité représentant la distribution locale de probabilité qui ne dépend que de l'état des parents du nœud (les tables sont une représentation quantitative de la connaissance).

statique		inductif		qualitatif	
dynamique	✓	déductif	✓	quantitatif	✓

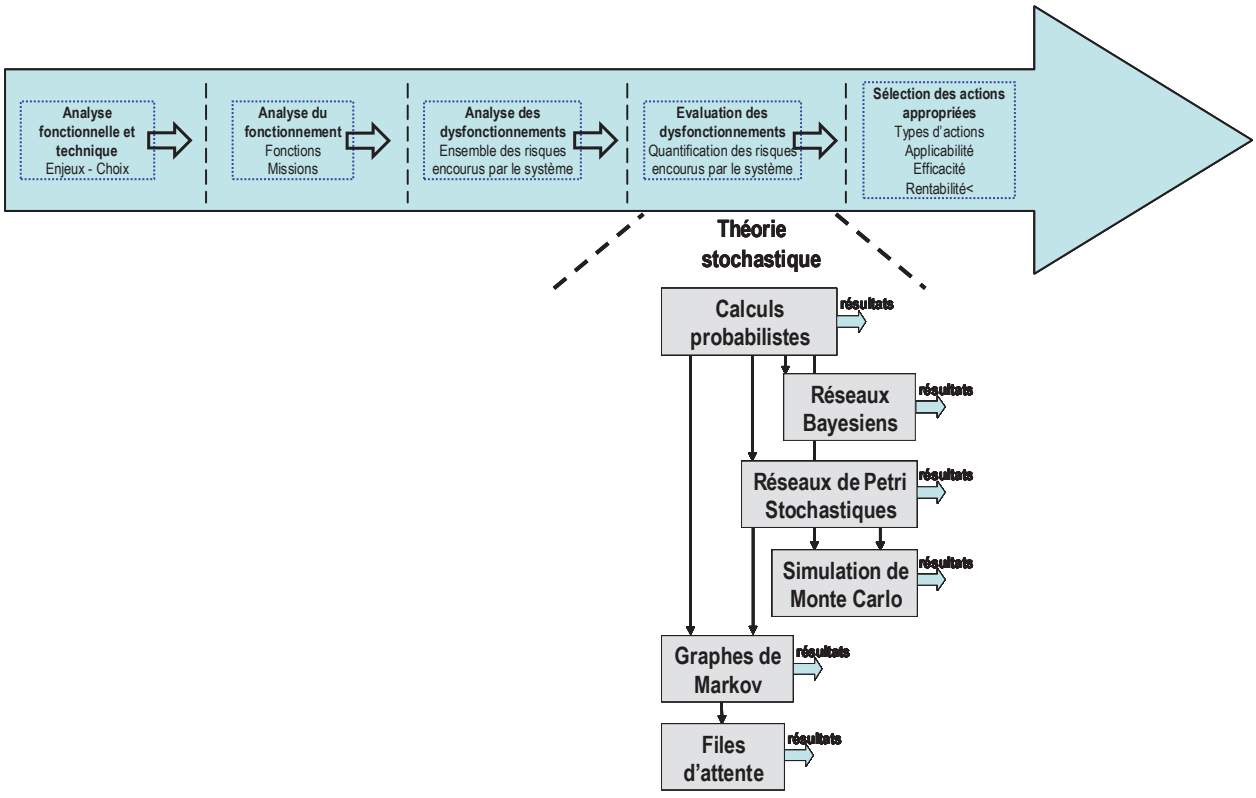


Figure 13 - Outils de la théorie stochastique

. Réseaux de Petri Stochastiques (RdPS)
Les RdP sont un outil d'analyse de la structure et du comportement des systèmes dynamiques à événements discrets.
Basés sur la description des relations existant entre les conditions et les évènements intervenant sur le système, ils s'appuient sur une représentation mathématique qui s'ouvre à différentes formes d'analyse.
De nombreux travaux et ouvrages exposent les caractéristiques des RdP et les principales extensions auxquelles ils ont donné lieu. Citons, parmi les dossiers des Techniques de l'Ingénieur qui leur sont consacrés, les références [17], [36], [37], [38].

Les RdP Stochastiques sont une extension des Réseaux de Petri pour lesquels est associée à chaque transition une variable aléatoire temporelle avec sa fonction de densité de probabilité.
Les RdPS permettent deux formes d'exploitation :

. l'analyse directe du graphe des marquages conséquents qui permet de caractériser les propriétés générales et spécifiques (analyse de points de vue) du modèle (le traitement du graphe de marquage est une analyse qualitative),

. l'exploitation du processus stochastique associé (Markovien, semi-markovien, avec points de régénération,…) qui permet d'évaluer le comportement en régime permanent et transitoire du modèle (fréquence moyenne de franchissement de transition (événement), temps moyen de séjour dans les états tangibles,…) ; cette approche est quantitative.

Les RdPS sont souvent couplés à la méthode de simulation de Monte-Carlo évoqué plus loin.

statique		inductif		qualitatif	✓
dynamique	✓	déductif	✓	quantitatif	✓

. Graphes de Markov (GM)
Les graphes de Markov sont une représentation des systèmes permettant de rendre compte de leur comportement en tenant compte des dépendances entre leurs éléments constitutifs. L'approche est basée sur l'identification des différents états du système (Méthode de l'Espace d'Etats [23]) et l'analyse de la dynamique d'évolution entre ces états.
Ici encore, différents ouvrages et articles sont disponibles [39], [40]

Les sommets du graphe correspondant aux différents états du système ; les sommets sont reliés par des arcs valués à l'aide de taux (ou de probabilités) de transition non nuls associés aux évènements correspondant aux conditions de passage (les transitions) qui font évoluer le système d'un état à un autre.
Les graphes de Markov sont couramment utilisés pour étudier la fiabilité des systèmes réparables [41].
Le modèle associe une représentation graphique et son écriture matricielle (matrice de transition). Les traitements relèvent de calcul matriciel à partir de l'équation de Chapman Kolmogorov :

. à chaque instant t, la probabilité d'occupation d'un état du système ne dépend que la distribution initiale (à t=0) d'occupation des états et de la matrice de transition,

Les résultats sont quantitatifs : probabilités d'occupation d'états, fréquence d'événements,…, en régime transitoire ou permanent.
Une structure de coût (bénéfices, pénalités,…) peut-être associée aux temps d'occupation d'états ou aux événements déclencheurs de changement d'états permettant d'établir facilement différentes caractéristiques économiques.

statique		inductif		qualitatif	
dynamique	✓	déductif	✓	quantitatif	✓

Files d'attente (FE)
Les files d'attentes sont une forme de représentation et de traitement de problèmes stochastiques concernant les phénomènes d'attente [42].
Ce phénomène d'attente qui implique clients et serveurs peut être considéré dans des situations très diversifiées : systèmes bouclés, réseaux, (clients ré-entrants, coexistence de plusieurs serveurs et plusieurs files d'attente,…), règles de priorité,…. La théorie permet de prendre en compte et de modéliser les goulots d'étranglement dans les processus.
Les résultats sont essentiellement quantitatifs et portent sur le temps de séjour dans une file, la longueur de file,…

Simulation de Monte-Carlo (SMC)
La méthode est basée sur la simulation informatique de variables aléatoires. L'approche consiste à créer un grand nombre de scénarios en répétant l'attribution d'une valeur numérique à la (aux) variable(s) dépendant du déroulement des processus stochastiques puis à effectuer un traitement statistique des résultats successifs obtenus. : calcul de moyenne, de la dispersion,… sur la distribution de probabilités des résultats. L'ouvrage de Koller [43] constitue une bonne présentation de la méthode.

6 Conclusion

L'évaluation de performance des systèmes industriels est un élément essentiel du pilotage des entreprises dans leur recherche récurrente d'une plus grande compétitivité. La sûreté de fonctionnement est indissociable de cette performance des systèmes.
La sûreté de fonctionnement décrit et analyse les mécanismes qui conduisent aux incidents et défaillances des systèmes et propose et évalue les solutions à mettre en œuvre pour parer à ces problèmes.
Elle rend compte de l'aptitude du système à remplir sa mission et à résister aux défaillances matérielles, logicielles et humaines ainsi qu'aux agressions de son environnement et, en ceci, elle caractérise les performances d'un système, intervenant de façon majeure dans la réalisation de cette performance.

Une large panoplie d'outils est disponible tant en conception (pour robustifier le système et de maximiser le rapport performance/coût) qu'en exploitation (pour maintenir sa qualité de service et maîtriser les risques pouvant affecter son fonctionnement).

Les principaux représentants de ces outils ont été donnés avec leur positionnement dans la démarche générale d'action.

Bibliographie

[1] VESELY (W.E.), GOLDBERG (F.F.), ROBERTS (N.H.), HAASL (D.F.).- Fault tree Handbook. *U.S. Nuclear Regulatory Commission, Washington, 1981, USA*

[2] WALLISER B.- Systèmes et modèles. Introduction critique à l'analyse de systèmes. *Editions du Seuil, 1977*

[3] LE MOIGNE (J.L.).- La modélisation des systèmes complexes. *Ed. Dunod, 1999, Paris.*

[4] CLERGUE (G.).- L'apprentissage de la complexité. *Editions Hermes, 1977*

[5] AFIS.- L'ingénierie Système : un atout majeur pour la compétitivité des entreprises. *Actes de la 2ème Conférence Annuelle d'Ingénierie Système, Association Française d'Ingénierie Système, 2001*

[6] MORTUREUX (Y.).- La sûreté de fonctionnement : méthodes pour maîtriser les risques. *Techniques de l'Ingénieur, AG 4670, 2001*

[7] GIREAU (M.).- Sûreté de fonctionnement des systèmes - Principes et définitions. *Techniques de l'Ingénieur, E 3 850, 2005*

[8] HATOM (J.P.), HATON (M.C.). - Systèmes à base de connaissances. *Techniques de l'Ingénieur, H 3740, 2000*

[9] BRENIER (H.).- Les spécifications fonctionnelles. *Collection EEA, Editions Dunod, 2001*

[10] MATHERON (J.P.).- Comprendre Merise : outils conceptuels et organisationnels. *Editions Eyrolles, 2002*

[11] ROBOAM (M.).- La méthode Grai. Principes, outils, démarche et pratiques, Editions Teknea, 1993.

[12] TERRIER (F.), GERARD (S.).- UML pour le temps réel : le langage et les méthodes, *Techniques de l'Ingénieur, H 3740, 2000*

[13] BAUER (B.), ODELL (J.).- UML 2.0 and agents: how to build agent-based systems with the new UML standard, *Engineering Applications of Artificial Intelligence, vol. 18, pp. 141–157, mars 2005*

[14] LE COZ (E.).- Méthodes et outils de la qualité. Outils classiques. *Techniques de l'Ingénieur, AG 1770, 2001*

[15] CHEZE (N.).- Statistique inférentielle. Estimation. *Techniques de l'Ingénieur, AF 168, 2001*

[16] CROCHEMORE (S.).- Méthode Delphi. *Techniques de l'Ingénieur, AG 3740, 2005*

[17] LADET (P.).- Réseaux de Petri. *Techniques de l'Ingénieur, R 7252, 1989*

[18] BENETTO (E.).- Analyse du cycle de vie. Incertitudes des évaluations des impacts. *Techniques de l'Ingénieur, G 5620, 2005*

[19] LYONNET (P.).- La maintenance, mathématiques et méthodes. *Lavoisier, Tec & Doc, 1992*

[20] Dubois (D.), Prade (H.),- Théorie des possibilités. Applications à la représentation des connaissances en informatique, *Masson, Collection Méthode + Programme, 1988*

[21] ISO-IEC,- Risk management - Vocabulary - Guidelines for use in standards / Management du risque - Vocabulaire - Principes directeurs pour l'utilisation dans les normes. *ISO/IEC 2002*

[22] PERILHON (P.).- Mosar - Présentation de la méthode. *Techniques de l'Ingénieur, SE 4060, 2003*

[23] VILLEMEUR (A.). - Sûreté de fonctionnement des systèmes industriels. Fiabilité, facteurs humains, informatisation. *Collection de la Direction des Études et Recherches d'Électricité de France. Ed. Eyrolles, 1988, Paris.*

[24] BERGOT (M.), GRUDZIEN (L.). Sûreté et diagnostic des systèmes industriels. Principaux concepts, méthodes, techniques et outils, *Diagnostic et sûreté de fonctionnement*, vol. 5, n° 3, 1995.

[25] COURTOT (H.).- La gestion des risques dans les projets. *Maîtrise des risques et sûreté de fonctionnement des systèmes de production, Collection IC2, Hermès Science, 2002*

[26] PAGES (A), GONDRAN (M.).- Fiabilité des systèmes. *Collection Direction des Etudes et Recherches d'Electricité de France, Eyrolles, 1980*

[27] ZWINGELSTEIN (G.).- La maintenance basée sur la fiabilité. *Collection Diagnostic et Maintenance, Hermès, 1996*

[28] NIEL (E.).- Sécurité opérationnelle des systèmes de production. *Techniques de l'Ingénieur. R 7 640, 1997*

[29] SIGNORET (JP.).- Analyse des risques des systèmes dynamiques : préliminaires. *Techniques de l'Ingénieur, SE 4070, 2005*

[30] ZWINGELSTEIN (G.).- Sûreté de fonctionnement des systèmes industriels complexes. *Techniques de l'Ingénieur, S 8250, 1999*

[31] RIDOUX (M.).- AMDEC – Moyen. *Techniques de l'Ingénieur, AG 4 220, 1999*

[32] MORTUREUX (Y.).- Arbres de défaillance, des causes et d'événements. *Techniques de l'Ingénieur, SE 4050, 2002*

[33] MELEARD (S.).- Probabilités. Concepts fondamentaux. *Techniques de l'Ingénieur, AF 166, 2001*

[34] POIRIER (J.).- Table statistiques. *Techniques de l'Ingénieur. R 270,1992*

[35] NAÏM (P.), WUILLEMIN (P.),LERAY (P.),POURRET (O.),BECKER (A.).- Réseaux bayésiens, *Collection : Algorithmes. Editeur(s) : Eyrolles, 2004*

[36] RICHARD (P.), HARO (C.).- Applications des réseaux de Petri. *Techniques de l'Ingénieur, S 7254, 2001*

[37] COMBACAU (M.), ESTEBAN (P.), NKETSA (A.).- Commandes à réseaux de Petri. *Techniques de l'Ingénieur, S 7572, 2005*

[38] COMBACAU (M.), ESTEBAN (P.), NKETSA (A.).- Commandes à réseaux de Petri. Mise en œuvre et application. *Techniques de l'Ingénieur, S 7573, 2005*

[39] NOYES (D.).- Approche analytique par espace d'états : Markov. *Maîtrise des Risques et Sûreté de Fonctionnement des Systèmes de Production, Collection IC2, Hermès 2002*

[40] SIGNORET (JP.).- Analyse des risques des systèmes dynamiques : approche markovienne. *Techniques de l'Ingénieur, SE 4071, 2005*

[41] GIRAUD (M.).- Sûreté de fonctionnement des systèmes. Analyse des systèmes réparables. *Techniques de l'Ingénieur, E 3852, 2006*

[42] BAYNAT (B.).- Théorie des files d'attente. Des chaînes de Markov aux réseaux à forme produit. *Editions Hermès-Lavoisier, 2000*

[43] KOLLER (G.).- Risk assessment and Decision Making in Business and Industry. A practical Guide. *CRC Press LCC, 1999*